Seminar Komplexität und Kryptographie

Erzeugung und Verwendung von Zufall

Ablauf und Referatsthemen

Johannes Köbler Sebastian Kuhnert

Wintersemester 2010/11

Übersicht für heute

1. Themen
2. Ablauf des Seminars
3. Hinweise für Referate und Ausarbeitungen
4. Themen für Referate

Themen

- Pseudozufallsgeneratoren
- Einwegfunktionen
- Derandomisierung

Themen

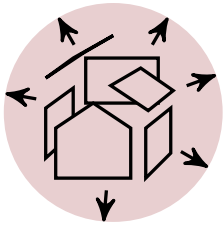
- Pseudozufallsgeneratoren
- Einwegfunktionen
- Derandomisierung

Themen

- Pseudozufallsgeneratoren
- Einwegfunktionen
- Derandomisierung

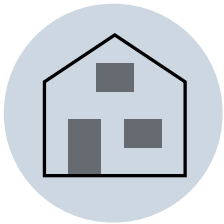
Übersicht für heute

Ablauf des Seminars



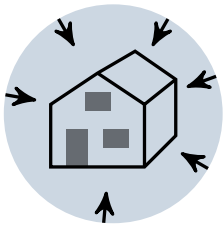
Thema auswählen

heute • Referate aussuchen



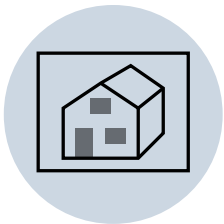
Referat vorbereiten

Literatur lesen • Thema erarbeiten



Referat halten

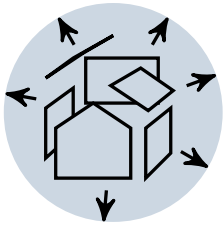
90 Minuten • da sein • nachfragen



Ausarbeitung schreiben

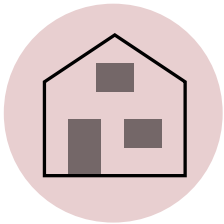
ca. 10-20 Seiten • Internet

Ablauf des Seminars



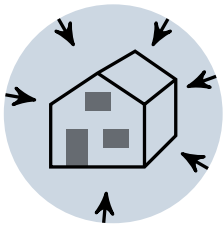
Thema auswählen

heute • Referate aussuchen



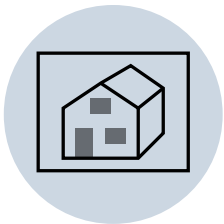
Referat vorbereiten

Literatur lesen • Thema erarbeiten



Referat halten

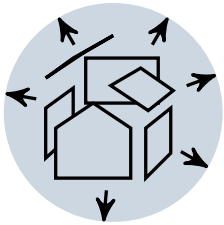
90 Minuten • da sein • nachfragen



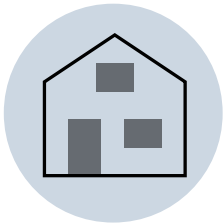
Ausarbeitung schreiben

ca. 10-20 Seiten • Internet

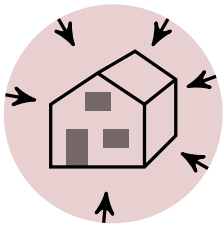
Ablauf des Seminars



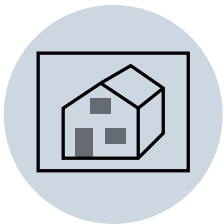
Thema auswählen
heute • Referate aussuchen



Referat vorbereiten
Literatur lesen • Thema erarbeiten

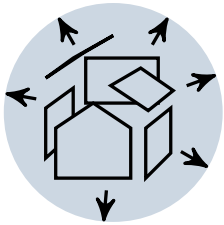


Referat halten
90 Minuten • da sein • nachfragen

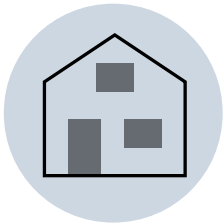


Ausarbeitung schreiben
ca. 10-20 Seiten • Internet

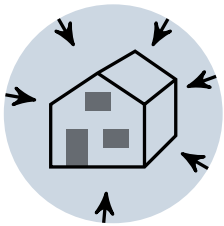
Ablauf des Seminars



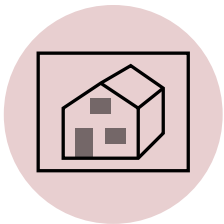
Thema auswählen
heute • Referate aussuchen



Referat vorbereiten
Literatur lesen • Thema erarbeiten



Referat halten
90 Minuten • da sein • nachfragen



Ausarbeitung schreiben
ca. 10-20 Seiten • Internet

Seminar »Erzeugung und Verwendung von Zufall«

Johannes Köbler, Sebastian Kuhnert

Übersicht für heute

1. Themen
2. Ablauf des Seminars
3. Hinweise für Referate und Ausarbeitungen
4. Themen für Referate

Eigenschaften eines guten Referats

- Ziele:
  - Ihr erarbeitet euch ein Thema selbst
  - Ihr vermittelt dieses Thema anderen
  - Ihr sammelt Vortragspraxis
- Aufbau:
  1. Einführung: Einordnung, Relevanz, Intuition
  2. Grundlagen: Definitionen, Konzepte
  3. Hauptteil: Sätze, Konstruktionen, Beweise
  4. Zusammenfassung und Ausblick
- Anschaulich
  - Nicht zu viel voraussetzen
  - Beispiele, Bilder
  - »Was hat mir geholfen, das zu verstehen?«
- Präzise
  - Klare Definitionen
  - Details von Konstruktionen und Beweisen

Eigenschaften eines guten Referats

- Ziele:
  - Ihr erarbeitet euch ein Thema selbst
  - Ihr vermittelt dieses Thema anderen
  - Ihr sammelt Vortragspraxis
- Aufbau:
  1. Einführung: Einordnung, Relevanz, Intuition
  2. Grundlagen: Definitionen, Konzepte
  3. Hauptteil: Sätze, Konstruktionen, Beweise
  4. Zusammenfassung und Ausblick
- Anschaulich
  - Nicht zu viel voraussetzen
  - Beispiele, Bilder
  - »Was hat mir geholfen, das zu verstehen?«
- Präzise
  - Klare Definitionen
  - Details von Konstruktionen und Beweisen

Eigenschaften eines guten Referats

- Ziele:
  - Ihr erarbeitet euch ein Thema selbst
  - Ihr vermittelt dieses Thema anderen
  - Ihr sammelt Vortragspraxis
- Aufbau:
  1. Einführung: Einordnung, Relevanz, Intuition
  2. Grundlagen: Definitionen, Konzepte
  3. Hauptteil: Sätze, Konstruktionen, Beweise
  4. Zusammenfassung und Ausblick
- Anschaulich
  - Nicht zu viel voraussetzen
  - Beispiele, Bilder
  - »Was hat mir geholfen, das zu verstehen?«
- Präzise
  - Klare Definitionen
  - Details von Konstruktionen und Beweisen

Eigenschaften eines guten Referats

- Ziele:
  - Ihr erarbeitet euch ein Thema selbst
  - Ihr vermittelt dieses Thema anderen
  - Ihr sammelt Vortragspraxis
- Aufbau:
  1. Einführung: Einordnung, Relevanz, Intuition
  2. Grundlagen: Definitionen, Konzepte
  3. Hauptteil: Sätze, Konstruktionen, Beweise
  4. Zusammenfassung und Ausblick
- Anschaulich
  - Nicht zu viel voraussetzen
  - Beispiele, Bilder
  - »Was hat mir geholfen, das zu verstehen?«
- Präzise
  - Klare Definitionen
  - Details von Konstruktionen und Beweisen

Der Weg zu einem guten Referat

- Arbeitsschritte:
  1. Einarbeiten
     - Literatur beschaffen und lesen
     - Notizen machen
  2. Vortrag erarbeiten
     - Struktur
     - Folien, Tafelbild
  3. Sprechstunde nutzen
     - 1–2 Wochen vor dem Referat
  4. Vortrag proben
     - Zeit abschätzen
     - Sicherheit gewinnen
- Bewährte Medienwahl:
  - Beamer für Definitionen und Sätze
  - Tafel für Beispiele und Beweise

Hinweise für Ausarbeitungen

- Aufbau:
  1. Titel, Autor, Datum, Name des Seminars
  2. Einleitung
  3. Grundlagen
  4. Hauptteil
  5. Zusammenfassung und Ausblick
  6. Literaturverzeichnis
- Arbeitsschritte:
  1. Vortrag ausformulieren
  2. Auf weiterführende Literatur verweisen
  3. Abgeben und Feedback abwarten
  4. Endgültige Version für die Webseite abgeben

Hinweise für Ausarbeitungen

- Aufbau:
  1. Titel, Autor, Datum, Name des Seminars
  2. Einleitung
  3. Grundlagen
  4. Hauptteil
  5. Zusammenfassung und Ausblick
  6. Literaturverzeichnis
- Arbeitsschritte:
  1. Vortrag ausformulieren
  2. Auf weiterführende Literatur verweisen
  3. Abgeben und Feedback abwarten
  4. Endgültige Version für die Webseite abgeben

Übersicht für heute

1. Themen
2. Ablauf des Seminars
3. Hinweise für Referate und Ausarbeitungen
4. Themen für Referate

Referat 1

Thema: **Äquivalenz der Existenz von schwachen und starken Einwegfunktionen.**
Schwache Einwegfunktionen sind manchmal schwer zu invertieren, starke Einwegfunktionen fast immer.

Inhalt: Wie sind Einwegfunktionen genau definiert? Wie kann aus einer schwachen Einwegfunktion eine starke konstruiert werden?

Literatur: Arora und Barak, *Computational complexity*, Kapitel 9, Goldreich, *Foundations of cryptography*, Kapitel 2

Referat 2

Thema: **Pseudozufallsgeneratoren: Ununterscheidbarkeit und Unvorhersagbarkeit.**
Ein Pseudozufallsgenerator ist eine Funktion, die aus einer kurzen, zufällig zu wählenden Eingabe eine längere, zufällig aussehende Ausgabe berechnet.

Inhalt: Wie können Pseudozufallsgeneratoren durch Ununterscheidbarkeit und Unvorhersagbarkeit definiert werden? Warum sind beide Definitionen äquivalent?

Literatur: Arora und Barak, *Computational complexity*, Kapitel 9

Referat 3

Thema: **Äquivalenz der Existenz von Einwegfunktionen und Pseudozufallsgeneratoren.**

Inhalt: Warum gibt es genau dann Einwegfunktionen, wenn es Pseudozufallsgeneratoren gibt?

Literatur: Arora und Barak, *Computational complexity*, Kapitel 9

Referat 4

Thema: **Derandomisierung von probabilistischen Komplexitätsklassen.**
Neben der Komplexitätsklasse P, die effiziente deterministische Berechenbarkeit charakterisiert, hat sich die Klasse BPP zur Beschreibung von effizienten probabilistischen Berechnungen etabliert.

Inhalt: Wie ist BPP genau definiert? Unter welchen Voraussetzungen kann $\mathrm{BPP} = \mathrm{P}$ gezeigt werden?

Literatur: Arora und Barak, *Computational complexity*, Kapitel 7 und 20

Referat 5

Thema: **Extraktoren** können selbst aus nur schwach zufälligen Quellen brauchbare Zufallszahlen erzeugen.

Inhalt: Wie lassen sich Extraktoren genau definieren? Wie können sie konstruiert werden? Wie können sie zur Derandomisierung verwendet werden?

Literatur: Arora und Barak, *Computational complexity*, Kapitel 20

Referat 6

Thema: **Elektronisches Geld.**

Inhalt: Wie kann durch kryptographische Methoden beim Bezahlen im Internet die von Bargeld gewohnte Anonymität hergestellt werden, ohne dass digitale »Münzen« beliebig kopiert werden können?

Literatur: Mollin, *RSA and public key cryptography*, Kapitel 7, Trappe und Washington, *Introduction to cryptography with coding theory*, Kapitel 11

Übersicht über Referate

1. Äquivalenz der Existenz von schwachen und starken Einwegfunktionen
2. Pseudozufallsgeneratoren: Ununterscheidbarkeit und Unvorhersagbarkeit
3. Äquivalenz der Existenz von Einwegfunktionen und Pseudozufallsgeneratoren
4. Derandomisierung von probabilistischen Komplexitätsklassen
5. Extraktoren
6. Elektronisches Geld